Reference to this paper in APA (6th):

Sunde, I. M. (2016). A new thing under the sun?: Crime in the digitized society. I A. Kinnunen (Ed.), *NSfK's 58. Research Seminar: New challenges in criminology: Can old theories be used to explain or understand new crimes?* (p. 60-79). Bifröst: Scandinavian Research Counsil for Criminology.

This is the final text version of the article, it may contain minor differences from the publisher's pdf version.

A New Thing under the Sun? Crime in the Digitized Society.

Inger Marie Sunde, Professor (Ph.D).
The Norwegian Police University College/Politihøgskolen

1. Introduction to Crime in the Digitized Society

Computer systems can be used to commit – and be targets of – crime. The article investigates whether so-called *"digital crime"* can be regarded as a new thing under the sun. The question itself is not new. It was originally raised in the 1950ies when computer technology had become sufficiently advanced to be put into use by large financial corporations and insurance companies (McQuade 2006: 11). Concomitantly, the opportunity to commit computer fraud emerged, an opportunity not lost on insiders. As the era of network technology and mobile devices had not yet arrived, outsiders did not have easy access to corporately owned computers, thus they were practically excluded from committing computer crime. Since insider crime in such corporations was regarded as being "white collar", computer crime was perceived as a form of white collar crime.

After the emergence of the Internet, "cybercrime" came to the fore. The prefix "cyber" suggests that the criminal phenomenon occurs in a space different from where humans act and relate. The crime is perceived as remote and the link to a specific perpetrator seems vague and diffuse. Crime may therefore be deemed to have developed into a new and unprecedented form. Obviously the criteria according to which we deem a phenomenon to be new, determines the assessment. Two criteria seem to predicate the present conclusion, firstly that what matters is the facts of the crime (digital technology), secondly, that the facts (technology) can be regarded as new. Thus the reasoning is as follows: As the crime could not have materialized in this form in the pre-computer era, the criminal phenomenon is new.

Such reasoning is not only clouded, but also hazardous. Continued application of the logic entails a risk of gradually removing criminal liability away from the perpetrator. The more "intelligent" the computer (never mind that the intelligence is artificial), less is the blame on the individual. Ultimately, the robot is the criminal. The human is reduced to a servant who merely executes the robot's commands. In the event that we not accept to regard a robot as perpetrator, no crime has been committed at all, because there is no perpetrator.

Fortunately, the fundamentals of criminal law do not change solely by the emergence of new technology. As long as basic legal principles are maintained, crime is committed by individuals, period. A robot cannot incur criminal liability, because the commissioning of a crime requires the perpetrator to fulfill conditions regarding *mental state* at the time when the crime is committed (the condition *mens rea*). The main rule is that criminal liability re-

quires intent *(dolus*). Should a robot have been trained to choose between alternatives, the choice is still made by a program created by humans. And humans are responsible for their doings. For example, a small monkey trained to climb through windows and take away silver ware, is a tool utilized by its owner. Its owner is the criminal. This is clearly so even if the monkey makes choices, for instance, on a lazy day it might refuse to work. An "intelligent" lawn mower which cuts down a fragile newly planted apple tree cannot be held liable for vandalism, even if it "chose" to ignore the program which told it to move around hindrances. In the age of artificial intelligence one should be careful not to confuse *liability* with *controllability*. Machines that are set to work for criminal purposes are legally to be considered as tools. From a criminal law perspective controllability may raise problems *mens rea.* The critical fact would be whether the perpetrator *realized that the outcome of its actions could be unlawful, yet chose to carry on.* This modality of intent is known as *dolus eventualis,* and fulfills the condition *mens rea*. Undoubtedly, also a robot must be regarded as a tool, no matter how "headstrong" and hard to control it is. The human is still responsible, and may be held criminally liable (provided that the act performed by the robot is a criminal offence laid down in law).

Some may claim that a *cyborg* can incur criminal liability. A cyborg differs from a robot in that it is made of *organic material* (and grafted into a machine), whereas a robot is made of "dead" material. A cyborg is therefore perceived to be more "human like" than a robot. Actually, in combination with strong computing power and artificial intelligence, cyborgs are perceived to be "super-humans", even *superior* to humans. In relation to criminal liability, however, the material of which the machine is made (live versus dead material) is irrelevant. Robots and cyborgs alike are associated with intelligence, but by virtue of being machines any possibility of assuming criminal liability is excluded. At least this is the case *de lege lata.* One may also ask what kind of punishment would be fit for a robot/cyborg. Probably, here is a case for reintroducing medieval forms of punishment, such as mutilation and decapitation. Even "brain" paralysis could be an option, in the form of deleting the program that runs the "perpetrator".

Today the phenomenon which somewhat vaguely has become known as "digitization" is present in every dimension, sector and level of society. It is reflected in all forms of social discourse, it be colloquial, professional, academic or political, where expressions such as "big data", "automation", "robotics", "Internet of Things", "cloud computing" and "artificial intelligence" have become common. One can also tell by our media habits. Constant presence on social media is the norm, not to possess a smartphone an oddity and turning it off not an option. TV-programs about artificial intelligence seem to cause the kind of marvel formerly reserved for Sir Attenborough's wildlife explorations.

My feel is that the habit of adding "cyber" as prefix to "crime" soon will end. It will end just as we no longer emphasize that cars are vehicles that are able to move without the assistance of horses, or that light bulbs are powered by electricity. "Cyber-expressions" might

become hallmarks of a *transitory stage,* defined by the struggle of coming to grips with digitization's impact on society. In a perspective *de lege ferenda* however, issues relating to (criminal) liability for *lack of control* may become increasingly relevant and important. Such questions can be addressed both with regards to producers and users of automated digital devices.

In the end the relevant question is whether *crime in the digitized society* is a new thing under the sun or not. A question so general lends itself to a nuanced explorative approach. Definite answers are not to be expected from the brief analysis of this article. What follows is a description of themes and priorities in *current cybercrime research*, and some observations as to where existing theories may fall short of explaining digital crime. If the article inspires more cyber research, its goal has been reached.

The structure of the ensuing parts is as follows: First we need to describe the subject matter of our investigation (section 2). Then we take a look on the human factor of cybercrime, which allegedly has been a blind spot in cybercrime research (section 3). Thereafter follows an analysis divided into three parts (sections 4 to 6). Section 4 adresses the problem of attribution, which is the top research priority of Interpol's Cyber Research Agenda. Section 5 adresses the function of digital technology as a cross cutting crime enabler, and section 6 - the final part of the analysis – discusses phenomena that can be regarded as new. It is asserted that criminal law *de lege lata* may be considered as partly inadequate, at least with respect to *random digital crime*. As regards the facts, digital technology produces some effects that create considerable problems for crime prevention, criminal investigation and prosecution. There is also much to indicate that online privacy violations have more hard-hitting effects on its victims than their physical equivalents. Finally, the main findings and conclusions are summarized (section 7).

2. Defining the Phenomenon: Digital Crime

In the introduction the notion was rejected, that technology itself suffices as sole criterion for defining digital crime. But how then do we define the criminal phenomenon which is the subject matter of our investigation? *"All crime is cybercrime"* Europol claims, and points to the necessity of *"thinking 'digital' first"* (Europol 2014: 84). However, the claim can merely serve as a general starting point, because we still need to make clear if we are concerned with digital crime *as it is performed* or digital crime *as defined in law*. The alternatives represent research topics relevant to criminology (crime as fact) and to law (crime as normative concept). In the former case we need to describe *which facts* that must be present in order for the crime to be a "cybercrime", whereas in the latter, we need to describe *the legal conditions* that define the crime as "digital" (a "cybercrime"). It turns out however, that the alternatives are both necessary, and must be combined. This can be explained as follows:

Crime as fact may take *the form of speech*. Common examples are threats of violence, fraudulent misrepresentation of facts, hate speech and distribution of sexual abuse material of

children. Crime in the form of speech can be committed *physically*, i.e., face to face ("F2F"), in a letter and so forth. Obviously such crime can also be committed *electronically*, for instance, a threat by email, skype or sms; a fraudulent website selling fake tickets to Premier League soccer games; a misleading website in a "phishing "scheme; hate speech on extremist fora, and; exchange of illegal images on the Darknet. Judged by *the facts* the "F2F-crimes" do *not* count as cybercrime, whereas their digital equivalents do.

The law however may not make relevant the distinction between speech F2F and its digital equivalent. Perfectly technology neutral criminal provisions may be *equally applicable to F2F crime and cybercrime.* Section 371 (a) of the Norwegian Criminal Code is an example in point. The provision concerns fraud by deception for the purpose of obtaining unlawful economic gain. The criminal offence is defined as the *fraudulent exploitation of a mistake made by the victim, who is brought in error by materially misleading information provided by the perpetrator*. Whether the act is performed F2F (for instance in a supermarket) or online (for instance in a webshop), is not relevant to the question of criminal liability, as the provision does not mention "cyber", "computer data", "digital" or the like. Yet the provision is very practical in relation to Internet fraud.

Conversely, it is conceivable that a reprehensible act performed online is not criminal, even if its physical equivalent is. The "blog case" from 2012 illustrates this (HR-2012-1554-U). Exhortations to kill two police officers were posted on a publicly available blog. Utterances with such content are punishable provided that they are made "in public". The Norwegian Supreme Court found that a blog could *not* be a forum for utterances made "in public" within the meaning of the criminal code. Had the exhortations been published in a physical newspaper instead, they would have constituted a crime.

The blog-case uncovered a legal anomaly, which led to an amendment of the legal provision also to cover utterances on the Internet. The legal definition is technology neutral, and the condition is that the utterance must "be suitable to be reached by a large number of people". 20-30 individuals suffice as "a large number". Because of the low threshold, most content on the Internet is made "in public" pursuant to Norwegian criminal law (Sunde 2016 chapter 3.2).

Finally, one cannot always be sure if digital and physical phenomena are legal equivalents or not. This can be illustrated by the uncertainty with regards to *the legal status of computer data*. According to Norwegian criminal law doctrine, computer data is *not* regarded as an "object". This is the case despite that computer data can be specified, individualized and quantified (factual aspects), and despite that one would think that the word "object" is technology neutral (legal interpretation). Unlawful deletion and suppression of computer data cannot, for this reason, be punished as traditional vandalism (i.e., vandalism against an object). The legislator has therefore been compelled to supplement the criminal provision with a new paragraph which specifically makes vandalism against computer data a criminal offence as well (Sunde 2006 chapter 4; 2011 chapters 6-10; 2016 chapter 2.5 and 6).

The examples show that an adequate definition of digital crime hardly can be attained by the sole application of factual or legal criteria. In order to ensure that the phenomenon we investigate is criminal and involves digital technology, conditions must be set relating *both* to law and to fact, as follows:

(i) The act must be covered by a criminal provision in force at the time when the crime was committed (the criminal provision may be technology neutral).
(ii) The act must involve - have a nexus with – digital technology.

By default, criminal acts which are covered by *technology specific* criminal provisions are included. Criminal provisions of this category typically concern computer intrusion, vandalism against computer data, computer forgery and computer fraud. Note that *computer fraud* is a crime different from *fraud by deception*, also when the latter is committed on the Internet. Computer fraud is defined as unlawful manipulation which *causes a computer automatically to perform a process* which entails an economic loss to somebody, (and is performed with the intent of obtaining an unlawful economic gain). The distinction between computer fraud and fraud by deception is that, a computer is *manipulated*, whereas an individual is *deceived* (can also happen on the Internet) (Sunde 2016, chapter 7).

A digression in furtherance of the note on robots and cyborgs: Fraudulent manipulation of a robot/cyborg is an instance of *computer fraud*. Despite their "intelligence", they cannot be "deceived" within the meaning of criminal law. Legally, *deception* indicates *a mental state exclusively reserved for humans*. *Speech* is a similar example. Legally, speech is a phenomenon *between humans*. An utterance which orders "sit!" is not speech if directed to a dog, yet it is if directed to a person. Voice transmission of login credentials to a computer is not speech, yet it is if uttered to an individual. The examples show that legal concepts developed to regulate inter-human behavior, may not be applicable to relations of a different kind (human-machine; human-animal). Neglect of the distinction between the *legal* meaning of words, and their practical (colloquial) meaning, may not only cause an analysis *de lege lata* to be flawed, but *undermine concepts important to criminal policy as well*.

On this backdrop the criteria for *digital crime* can be developed like this:

(i) The act must be covered by a criminal provision in force at the time when the crime was committed (the criminal provision may be technology neutral), and the act must involve digital technology.
(ii) If the criminal provision contains technology specific conditions (concerning digital technology), the acts falling under its scope are by default "digital" crime.

On a first glance, *physical crime* is excluded from the list, which means that crimes in the form of "F2F speech", arson, burglary, physical violence and homicide fall beyond the scope of our investigation. Or, is it really so? How about the Internet of Things ("IoT")? "Internet of Things" means that physical objects, living creatures and individuals, get connect-

ed to the Internet. Embeddables and wearables are integrated into or fixed onto the object / creature /individual, and put it online. The device can be contacted remotely (online), and be caused to do something (actuate). Actuation may have an impact on the object / creature / individual. The lesson learned from Internet connectivity is that, *in order to communicate, one must also expose oneself (the computer) to input* received from over the network. Input is not 100% controllable. Hence communication makes one vulnerable to abuse and attacks. This makes a case for questioning if indeed we succeeded in our efforts to single out a rational definition for *digital crime*.

Here are some examples of "IoT-crime":

(i) The online door lock

Electronic door locks controlled and managed online, have become popular. The resident of the house enters into an agreement with a door lock service provider (DSP). The DSP opens a user account for the resident, who becomes a door lock service subscriber. By managing the account, individual entrance codes can be set for each member of the household. Moreover, temporary entrance codes can be registered both for infrequent occacions (for instance letting in a babysitter) and for routine visits (for instance a biweekly house cleaning service). Each one has a unique code, so, should somebody else use it, the trusted holder of the code is responsible. Each usage of the entrance code is recorded in the logs of the user account with the DSP. However, assuming that the entrance codes are kept secret, the resident's security depends on the security of the DSP. The system of the DSP can be hacked and the entrance codes disabled or copied. A criminal organization, perhaps assisted by an insider, could disable the entrance codes of an entire neighborhood, or add their own codes, thus being able to empty the area before noon. The example describes a series of criminal offences, ranging from clear cut digital crime in the form of computer intrusion (hacking a DSP system) and vandalism against computer data (change/deletion of entrance codes), to physical crime (burglary). The burglary is facilitated by the preceding digital crimes. Should it too be considered as digital crime, or is it simply crime in the digitized society?

(ii) The online pacemaker

A corresponding scenario can be envisaged for online pacemakers, i.e., pacemakers monitored and updated over the Internet. The computer system of the pacemaker service provider can be hacked, and the electronic communication which supports the device can be interfered with. Worst case is a hack or interference which amounts to homicide. Perhaps we do not think of this as digital crime, but certainly it is crime in the digitized society.

Marie Moe, a 37 year old computer engineer, became acutely aware of the security issues relating to remote interference, when suddenly she needed a pacemaker. In an interview

with a Norwegian newspaper, she said she was prepared to be a more demanding customer in the future when her pacemaker needs replacement.[1]

In the end, we have to conclude that technological development expands our phenomenon, as also crimes such as burglary and homicide can involve *digital technology as a fact*, and the applicable *criminal provisions are technology neutral*. Europol's claim may therefore prove to be true. A practical effect is that *digital evidence* feature regularly, and must be secured as a matter of routine, in the course of a criminal investigation. Hence, knowledge and skills to secure and analyze such evidence are needed among criminal investigators no matter the type of crime they are tasked to deal with.

3. The Human Factor of Cybercrime – a Blind Spot

Crime is performed by individuals, notwithstanding any presence of digital features. The human factor of current digital crime has however to some extent been overlooked. At least this is the case if we are to believe Europol, which goes so far as to claim that the role of the individual has been "a blind spot" in cybercrime research (Europol 2014: 82). The explanation is that cybercrime primarily has been associated with threats against cyber- and information security, something which has entailed a strong focus on technical measures. From the perspective of the law enforcement, this approach is too narrow. Europol's message thus is that "*research focusing on people is vital if we have any real hope of coming to grips with the phenomena of computer crime*" (ibid). The police organization of the European Union is an important voice in this respect. It hosts the European Cybercrime Center - the "EC3" –, has sophisticated multidisciplinary competence, and has proved its ability to work quite efficiently against cybercrime.

The need for more research regarding the human factor of digital crime is not in dispute here. But this is not to say that one has been wholly oblivious of the human factor of cybercrime up until now. For instance, the significance of *social engineering* to cybercrime has always been emphasized. The problem of "phishing" is illuminating. The criminal set up is the making of a request – on a fake web site or in an email - to update your personal and financial data and access codes. The request appears to come from your bank or telecom provider, but is actually part of a scam. The information provided by the victim in response to the request, is used to empty the bank account, hack the email account, hire a car, take up a loan, receive social benefits and go shopping, just to mention some of the risks. All acts are performed in the name of the victim and/or against the victim's assets. The acts can take place offline and online, anywhere in the world, no matter where the victim lives.

Similarly, fraudulent deception can be based on social engineering. Currently, so-called "CEO-fraud" is a problem. The scam is performed by submitting an email to a subordinate

[1] «De medisinske hackerne», Dagens Næringsliv 8.1.16.
http://www.dn.no/magasinet/2016/01/08/2128/Teknologi/de-medisinske-hackerne

in a corporation. The email appears as sent from the CEO, who orders prompt effectuation of a big payment on behalf of the corporation. The subordinate dares not object or ask any questions, and carries out the instruction, whereupon the money ends in a bank account controlled by the criminals. According to an alert by the FBI, such scams have resulted in losses totalling more than USD 2 billion over a three year period.[2]

In terms of substantive criminal law "phishing" involves a series of criminal offences, comprising identity infringement, theft, computer intrusion, fraud, forgery and acquisition of access codes for the purpose of committing a crime against computer systems or computer data. The scheme as such is often referred to as "Identity theft" (ID-theft), and conceptually divided into the stages of (i) identity information harvesting; (ii) possession and disposal of identity information; and (iii) the use of identity information to commit fraud or other crimes (Cybercrime Convention Committee 2013: # 4; Wall 2014). The purpose is primarily to unlawfully gain profits or information based on usage of the victim's credentials. Victims are picked at random. Those who are vulnerable may be victimized.

Granted, Europol still has a point. But for issuing warnings and alerts against phishing and other forms of criminal social engineering, the practical response against cybercrime has primarily been technical, in the form of patches & updates, firewalls and so forth. Seemingly the need for research concerns, first of all, how to realize what it is exactly – with respect to behaviour – that we need to understand better, in order to explain why people become involved in digital crime. More precisely, we want to find out whether people get involved in online crime more easily than in "physical" crime, and if so, identify the causes and the effects. One important question is whether digitization brings about more crime than before, or merely moves crime from a physical arena to a digital.

Having succeeded in putting the human factor on the agenda, Europol follows up with sections that deal with *Profiling cybercriminals* and *Behaviour in cyberspace* (Europol 2014). The most relevant "cyber-psychological concepts" are claimed to be:

- Anonymity and self-disclosure
- Cyber immersion / presence
- Self-presentation online
- Pseudoparadoxical privacy
- Escalation online
- Impulsivity and problematic Internet use
- Dark tetrad of personality.

[2] "FBI warns of dramatic increase in business e-mail scams" (4.4.16). https://www.fbi.gov/phoenix/press-releases/2016. See also the blog Krebs on Security (16.4.16) http://krebsonsecurity.com/tag/ceo-fraud/. The loss estimate concerns scams reported in 79 countries in the period 2013-16.

This is not the place for further exploration of cyber-psychological concepts. However, assuming that "dark tetrad" is not an altogether familiar expression, the reader might be interested to learn that it is an expansion of the allegedly more well-known psychological phenomenon **"**dark triad" of personalities. A dark triad personality is regarded as *malevolent*, because it is "Machiavellian", "narcissistic" *and* "psychopathic". In Greek "tetrad" means "four", so the "dark tetrad of personalities" signifies an individual who possesses *yet another dark personality* (in addition to the three already mentioned). This is *sadism* (Buckels, Trapnell and Paulhus, 2014). Thus one may assume a "dark tetrad" to be *super-malevolent,* and only the imagination sets the limits for what such a person conceivably can be up to.

The research concerned "dark tetrads" is based on interviews with respondents from the United States. It turns out that those who fulfil the psychological criteria are so called "Internet trolls". In Norway, we tend to think of Internet trolls as bad-tempered people who provoke argument for the fun of it. "Trolling" can also be associated with "the deep voice" of the people, mercilessly asserting its right to *"to tell the truth exactly as it is".* Thus, in a Norwegian context, to associate Internet trolls with *sadism* could therefore be deemed as going a bit too far.Be that as it may, the reader may want to check it out for herself. To conclude: *"Trolls just want to have fun"*, at least, that's what the researchers say (ibid).

4. Interpol's Top Research Priority and Its Implications

The question still remains; is crime which involves digital technology a new thing under the sun or not? For the remaining part of the analysis *the top research priority* identified in Interpol's Cyber Research Agenda, is suitable as starting point. The priority has been agreed *between important stakeholders* who recognize the need for a knowledge based approach to digital crime (Interpol 2015). An intolerable level of digital crime endangers the benefits of digital technology, prosperity and safety of the society as a whole. Knowledge of the problem which is perceived to be the greatest, and most deserving of research in order to counter digital crime, may be helpful to our analysis.

The Interpol Cyber Research Agenda is the outcome of a workshop which convened *"an equal number of participants"* from the law enforcement, academia, private sector and public policy making bodies. Eight research themes were discussed: (1) Digital forensics; (2) Measuring and forecasting cybercrime; (3) Improving attribution; (4) Improving cyber hygiene; (5) Capacity building & training; (7) Improving information exchange and sharing; and (8) Cyber criminology. At the end, their relative importance was ranked by each of the four participating groups (ibid.).

"Improving Attribution" is the clear winner among the eight research themes. It is the top priority of the law enforcement, and second and third of the private sector and the policy makers. (Academia put cyber criminology on top).

"Improving Attribution" is short for *improving the law enforcement's ability and possibility to link a criminal act on the Internet to a specific individual who can be identified and held criminally liable (given that the legal conditions for criminal liability are fulfilled).*

It demonstrates a general agreement that *anonymity* is the major problem to prevention and prosecution of digital crime. Despite that the police may be aware of illegal activity online it can be unable, by regular methods, to identify the perpetrators. In order to convict somebody for a crime, evidence that links the perpetrator to the criminal act is required. The public prosecutor has the burden of proof, and must prove the link beyond any reasonable doubt. Under the protective shield of anonymity criminals can carry out illegal activities online with little risk of being caught. The risk is low, not non-existent. But, in order to identify criminals on anonymous services, the police may have to make use of so-called "extraordinary" or "untraditional" methods. Such methods are less controllable than the traditional ones. Undercover operations which infiltrate illegal market places may for instance entail a need to engage in illegal transactions. Observation of illegal activities without taking any intervening steps (in wait for "bigger fish"), raises ethical questions. Provocation may jeopardize prosecution, and should evidence be deemed as unlawfully obtained the risk is that it is excluded from trial.

The TOR network ("The Onion Router" network) is the most well-known anonymous network. Computers running the TOR-software are nodes that function as layers ("onion layers"). Their purpose is to anonymize communication by "shaving off" information that identifies its source. "Darknet" is frequently used as synonym to TOR (which is not totally fair to TOR, but that is a different story). "Darknet" is the illegal part of the "Deep web". The Deep web is the part of the Internet which is not indexed by ordinary search engines. *The source* of the communication on the Darknet is usually hidden (anonymous). In addition, *the content* of the communication can be encrypted. Problems of anonymity and encryption are among the driving forces behind increasingly more intrusive investigation methods. Computer surveillance is an example in point. The method became legally authorized and sanctioned by the Norwegian legislator in June 2016 after seven years of deliberation.[3]

The TOR network itself can of course be technologically infiltrated by nodes controlled by the law enforcement. Should the practice become popular, a risk of running into "blue on blue" operations – where police organisations go after each other, instead of after the criminals – cannot be ignored.

[3] Computer surveillance is "dataavlesing" in Norwegian. An expert committee proposed the method in 2009 in the report "Hidden information – Open control" (my translation from Norwegian) (Metodekontrollutvalget 2009). The result is a new chapter 16d (computer surveillance) in the Norwegian Criminal Procedural Code, adopted by law no 54/2016 of 17 June 2016.

Moreover, not only communication, but also *payments* can be performed anonymously. The usage of block chain currency, of which Bitcoin is the most well-known, sees to this. According to Europol's stats, Bitcoin accounts for 40% of all identified criminal-to-criminal payments in the EU. It features as *"a common payment mechanism across all [criminal] payment scenarios"*. Europol concludes that Bitcoin is establishing itself as *"a single common currency for cybercriminals within the EU"* (Europol 2015: 11, 46-47).

Computer engineers and other technical experts often take measure of the probability that algorithms which provide anonymity can be mathematically cracked. Hence, they prefer the word "pseudonymity". From a practitioner's point of view, mathematical probability calculation is one thing and practical investigation quite another. Both TOR and Bitcoin are services that provide anonymity for practical purposes. Some claim that Bitcoin is not anonymous because the transactions are recorded and made transparent in the publicly available block chain log (e.g. Meiklejohn, Pomarole, Jordan et. al., 2013). But even if the log may contain sufficient information to deduce the identity of certain big "Bitcoin players", it *does not plainly disclose specific identity information*. The anonymity of its users might perhaps not survive a dedicated mathematical attack, but so far the digital currency has preserved sufficient unallocated blocks to shield the user's identity from the investigative eye of the law enforcement.

Given the significance of the problem, research concerning "Improving Attribution" must be important. Whether the outcome supports a strategy which aims at cracking the anonymity of criminals (and of everybody else), or just pave the way for other strategies, remain an open question. It is important whether policy makers are dedicated to strategies of general deterrent effects, or prefer other strategies. In any case, anonymity as problem number one does not give any reason for questioning old theories that can explain crime, or throw them overboard. Rather, the situation is the opposite. Traditional key factors of crime such as economic gain, opportunity and low risk are clearly present in digital crime. Anonymity facilitates and enhances them all.

5. Digital Technology as a Cross Cutting Crime Enabler

So far, the most striking observation of the analysis is that *new technology is relevant to a wide range of crimes*. Europol has captured this nicely by pointing out that digital services function as *"cross cutting crime enablers"* (Europol 2015: 15). Digital technology is generally relevant to and facilitates crime, no matter the type of crime. Digital technology offers functions and services which make life easier, enable public administration to operate more efficiently and commerce to be more competitive. The flip side of the coin is that criminals may exploit its benefits equally well. Besides from *"money mules and money laundering services"* Europol's list of cross cutting crime enablers thus feature *"bullet proof hosting"*, *"illegal trading sites on the Darknet"*, *"criminal schemes around Bitcoin and other virtual currencies"* and *"criminal expert forums online"* (ibid.).

The upshot is that crime has become an online service. One can seek the service of a criminal host, get illegal advice, hacker tools, illegal content, drugs, devices such as explosives and firearms, and even hire a hitman, on demand. The host can hold Bitcoin in escrow, providing a safe mechanism for the exchange of a criminal service against payment. According to Europol, "Crime-as-a-Sevice" ("CaaS") *"acts as a multiplier for many facets of cybercrime. Services such as bulletproof hosting, spam, illegal currency exchanges, money mules and counter anti-virus […] may have been crucial to those offences being committed"* (Europol 2015: 63, see also p.7).

CaaS mirrors ordinary online commerce. However, while law-abiding services adhere to rules for bookkeeping and accounting, knowing your customer, the conditions for a license (for instance to sell fire arms or sell pharmaceuticals), CaaS operates outside the legal regulatory framework, and outside the law. CaaS operates in a normative environment where it is understood that the activity is illegal, hence the participants take care to operate anonymously.

Finally, one may point to the leveraging effect of network technology. It has caused criminologists to question the methods for defining and quantifying online crime, the adequacy of current theories of digital victimization, and the methods according to which economic losses and damages are calculated (e.g. Wall 2007). The examples in point concern dissemination of computer virus which may infect thousands, even millions, of computers in a short time; the perennial availability of illegal content on the Internet, and the estimates of economic loss (should it be recoverable, because it is caused by a crime, or just as an instance of bad luck no different from the risk we take in other aspects of life?). The questions are open for research.

6. Things that can be regarded as New under the Sun

In this section we turn to criminal phenomena which can be regarded as new, either because of law or of fact. As regards the law, it can be asserted that it does not adequately grasp the significance of network technology to crime. Important effects of *connectivity* have yet to be suitably taken account of by criminal law. As regards the facts, it can be asserted that the effects of *automation* and *online privacy violations* raise serious questions, which cause problems that can be regarded as new.

6.1 Internet Connectivity vs. the Notion of a Direct Attack

Internet Banking Fraud, cyber-extortion and DDOS-attacks may be performed according to largely similar *modus operandi*. Below, Internet banking fraud is presented as the "case". Chronologically the events succeed as follows:

Step one, *the developing phase*, is concerned with the development of a program (malware) which can be remotely controlled. Step two, *the distribution phase*, is concerned with the in-

fection of computers. Infection is caused either from popular websites where the malware has been stealthily placed, or in the form of spam-mail with a malware attachment. Victimization is random. Those who own a computer vulnerable to the malware may get infected (nothing "personal" here). Step three, *the notification phase*: This is when the malware transmits an alert over the network to the perpetrator, informing about the identity of the infected computer, whereupon it becomes a target for the perpetrator. Step four, *the exploitation phase*: The perpetrator exploits the vulnerability. In the case of Internet banking fraud, he takes control over the victim's connection with the bank, and places a payment order to an account controlled by a so-called "money mule". At this point final success depends on two factors: Firstly, that the victim is tricked to confirm payment; secondly, that the money mule delivers the money (net of a provision), to the main perpetrator (the "main brain"). Accordingly, *the final step* is the *phase when the scheme is completed:* The victim is tricked to confirm payment from her account, because she is *asked to log in twice due to a fake error alert* caused by the malware. When she enters the secret key as part of the logon procedure, she unwittingly confirms the order. Promptly upon notice that its account has been credited, the loyal money mule withdraws the money in cash from an ATM. The proceeds are ultimately delivered to the "main brain".

One may note a certain discrepancy between the legal conceptualization and the practical implementation of the crime. The facts describe a *criminal continuum* in stark contrast to the *specificity of criminal provisions*. The specification is due partly to *the principle of legality*, partly to *tradition* and partly to *perception of the interests that is violated and must be protected*. *The principle of legality* protects individuals from arbitrary prosecution and punishment, by requiring that the law first must describe which acts that are criminal (cfr., e.g., ECHR article 7 and the Norwegian Constitution section 96). But the principle of legality does not give precise instruction as to how the description must be framed. This depends a lot on tradition and perception of the protected interest.

Currently, criminal law has split digital crime into a multitude of criminal offences. Examples in point are the making and/or distribution of malware, computer intrusion, illegal surveillance, interference with computer data, interference with computer systems, computer fraud and fraud by deception. This mode of thought stems from *tradition* and is reflected in the Cybercrime Convention (CETS 185). The convention has had considerable international influence. Criminal provisions of corresponding character are therefore generally included in the criminal codes in national legal systems. Finally, the protected interests are *privacy* and the *property* interests of the owner of the computer and the bank account. The owner is the offended party ("fornærmede").

The outcome of the legislative approach is that the owner of the computer is the victim of a multitude of crimes (computer intrusion, computer surveillance, vandalism against computer data and/or the computer system, computer fraud or fraud by deception). This is a bit odd, given that his computer *only is a vehicle to commit a crime, and has been picked at random.*

Typical for such crime is that the malware infects many computers, thus effectively creating *botnets* controlled by the criminal. That is why *modus operandi* largely is the same also for cyber-extortion and DDOS-attacks.

Cyber-extortion can be performed by infecting computers with malware which encrypts the content ("ransomware"/"cryptolocker"). Unless the owner pays an amount as ransom, in Bitcoin, within a certain deadline, the decryption key is deleted, hence the data is lost. Also DDOS-attacks (vandalism against computer systems) can be used for the purpose of extorting payment from a victim. The victim pays under the threat of else suffering a DDOS-attack. A DDOS-attack is usually carried out by triggering a botnet to attack the target computer. A simultaneous attack by thousands of computers brings down the target.

The creation and utilization of botnets through malware infection is a main feature of such crime. The botnet is a resource on the Internet, which in essence is about making computer resources available to others (e.g. supplying computing power for a decryption experiment). However, the exploitation of a botnet as described above is undoubtedly criminal. The point concerns *the distinction between targeted and random digital crime*. The *criminal modus operandi* described above, shows that *randomly chosen* Internet computers are used as *resources for a continuing widespread criminal activity*. The crime is not targeted at special victims. The law does not fully seem to capture this. Rather, it seems to be based on the opposite assumption.

The Cybercrime Convention Committee has observed that computers *"may be linked for criminal or good purposes […] The relevant factors are that the computers in botnets are used without consent and are used for criminal purposes and to cause major impact."* (Cybercrime Convention Committee # 2 (botnets). Cf. also # 3 (DDOS-attacks) and # 6 (malware).

Essentially, the problem concerns *victimization and the interests that are put at stake* by such crime. Legal policymakers have so far mainly concentrated on *modus operandi,* and paid less attention to the other questions. But they are at least as important to the framing of provisions of criminal law, as the modus operandi. One could envisage that the law, instead of featuring the computer owner as *the victim* of a crime, treated the crime as a violation of the public interest in information security. The crime could be described in terms of *a criminal continuum.* The number of infringements on confidentiality, integrity and availability, could be regarded as *aggravating circumstances*, in addition of course to the size of the illegal profits. Criminal provisions of this kind are applied in relation to terrorism and sabotage, and seem relevant to *ordinary random digital crime* as well. The computer/account owners may be indemnified by insurance coverage, refund from the bank and damages paid by the criminal or covered by proceeds that have been confiscated.

Bitcoin can be confiscated. In the case against the founder of "the online drug bazaar Silk Road" Ross Ulbricht, 144 000 Bitcoin was confiscated as proceeds from crime. In June 2016

when Australian law enforcement held a Bitcoin auction, the amount equalled more than USD 13 million (NOK 108 million).[4]

Existing criminal provisions should be maintained in so far as they are necessary to punish *crime which is targeted* at certain victims. This would be computer intrusion for the purpose of state or industrial espionage, computer interference for the purpose of bringing down a competitor, surveillance for the purpose of controlling the private life of an ex-girlfriend and so forth.

References to some cases concerning *random digital crime* prosecuted in Norwegian courts: Internet banking fraud: HR-20122-2397-A; DDOS-attack by botnet: TNERO-2013-89352; Random hacking: HR-2004-1807-A. *Targeted* hacking and vandalism against a competitor is the case in HR-2004-127-A. Information crime at the expense of a competitor is illustrated in TOSLO-2004-84792, and targeted search for intimate images in HR-2012-2056-A.

The approach may also be adequate to deal with IoT-crime (discussed in section 2). Burglary has been regarded as a crime against property and private life. But numerous house owners are put at risk, if the crime is pulled off first by hacking the computer system of the DSP (or of the cloud service that hosts the service of the DSP). The house owners are randomly picked according to the same criteria as the owner of the internet computer, and the crime is carried out by exploitation of network vulnerability.

A corresponding scenario is perhaps not as likely with respect to the pacemaker, because homicide usually is targeted. However, large-scale random killings are conceivable, as a terrorist attack. Killing is terrorist communication, it does not matter who the victims are. In the wake of the Charlie Hebdo killings, TV5 Monde France was taken down by hackers.[5] The hack was originally thought to have been performed by the "CyberCaliphate", i.e. hackers partial to IS., The assumption has later been questioned as new leads point to Russian hackers called "Pawn Storm".[6]

6.2 The impact of automation

Automation may be exploited to commit crime in a "self-executing" manner. This has several advantages to the perpetrator. The perpetrator's efforts are only needed in the initial phase of planning and of software development. The criminal concept could for instance be a fake website which sells tickets to Premier League soccer games. The website is connected to publicly available databases with information about time and location of the games.

[4] https://www.theguardian.com/technology/2016/may/31/australian-police-to-auction-13m-in-confiscated-bitcoins

[5] https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers

[6] http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html.

Thus the service is automatically updated with new events. Payment is made by card. The tickets obtained from the service are not valid of course.

When the program (website) is put to work, the perpetrator is free to move around, perhaps go on holiday and enjoy the proceeds which keep coming in as a steady flow to his bank account. Thus, automation provides new flexibility to the perpetrator, because there is no need to be present at a physical crime scene. The flexibility may be utilized to cross international borders, and increases the problems that the law enforcement already has to identify and locate the perpetrator. The scheme may be further enhanced by anonymity, both with regards to the Internet source of the fraudulent website, and the ownership of the bank account (client privilege in safe havens for banking services). Also the anonymity of Bitcoin can be exploited, for instance by cooperating with the host of a "bullet proof" service who holds the proceeds in escrow for a certain time.

There are early warnings that this type of fraud may become a problem. In Sweden, five men were convicted for fraud. They had developed the automated poker playing program "Maggie", which was put to play on Svenska Spel ("Swedish Games"), a site which was open for participation by real persons only. Maggie's poker playing skills were superior to the other players', and she beat more than 5000 players before the scam was uncovered. The court estimated their economic loss to SEK 760 000 (approximately EUR 80 000).[7]

6.3 The Sad Story of Criminal Privacy Infringements

Commercial live streaming of children is on the increase, facilitated by broadband and anonymity. The users pay in Bitcoin, and instruct the criminal in the other end, of the kind of abuse they want to watch. Here, the crime is carried out on demand, which makes it a genuine instance of CaaS. This worrying development of crime against children comes in addition to the burden of *the lifelong violation* against their privacy, caused by the perennial circulation of images of the abuse on the Internet. For more detail about this, see (Sunde 2011, and 2016 chapter 10.1).

There is also *stalking, harassment and sextortion*. "Sextortion" means that the victim is forced or threatened to give away personal sexual images or video clips. Teenagers and even younger children are particularly vulnerable to this kind of crime. Legally it is not regarded as *extortion*, because the victim does not suffer a loss in economic terms. Such crime is punished according to provisions regarding unlawfully to compel somebody to do something against its will, and unlawful threats. The unlawful invasion of the private sphere and consequent loss of intimate information is not fully recognized by such more or less "value neutral" provisions. Whether the current legal response is adequate in relation to the problem is an open question.

[7] Södertörn tingsrätts dom 2014-12-19, case number B 5929-13.

There is also much evidence to the effect that harassment on the Internet is more hard-hitting than harassment in physical space. The fate of the American teenager Amanda Todd has become a symbol of this. She committed suicide at the age of 15, after having been bullied on social media for years. The triggering event for the harassment is explained to be that she, at the age of 12, was deceived to give away intimate images to some "friends", who later shamed her by making them available on social media. Despite efforts to ameliorate the situation, change school etc., she was harassed. She finally made a video in which she explains how she had suffered and her decision to commit suicide. She posted the video clip on YouTube, then, ended her life.

The Norwegian "tech" journalist and author Per Kristian Bjørkeng explains why online harassment has greater detrimental effect to the victim, than harassment in physical space. Bjørkeng points out (i) the (perceived) need for constant online availability, which exposes vulnerability in terms of being prevented from protecting oneself from receiving unwanted messages; (ii) the effect of online anonymity and misuse of the identity of others. It may cause a situation where the victim cannot be sure who is behind the bullying. The possibility that someone in the victim's close social environment is the one, cannot be ruled out. A great sense of insecurity is thus created. If the fears prove to be true, the victim may totally lose confidence in others more generally. It is like the world comes to a crash; and finally (iii) the "one degree of separation" which means that regrettable actions easily can be made on impulse. A sharp message is now promptly submitted, by entering "send", when formerly one could normally sleep on it, and perhaps wake up in a friendlier mood. Separation also prevents the sender from watching the recipient's immediate reaction. It could be that the written message came out more aggressively than intended, or was misunderstood. In any case the sender is prevented from moderating the message, or offer an excuse, unless the victim actively seeks it (Bjørkeng 2011).

For these reasons, and in order to live up to the positive obligation to protect the right to private life, which flows from the EHRC article 8, the Norwegian criminal code has been supplemented with a new provision concerning serious stalking and harassment, i.e. section 266a. The crime can be punished with imprisonment for up to four years.

7. Concluding Remarks

The analysis has shown that it is difficult to make a clear distinction between digital and physical crime when both law and fact are taken into account. The better approach is to address *crime in the digitized society*, and be generally prepared for the *relevance of digital evidence to all kinds of crime*.

As regards the human factor, more research is needed in order to "come to grips with" digital crime. It is essential to find out whether there is a *decrease* of physical crime, while digital crime is on the increase. A more ominous possibility is that *crime overall* is on the in-

crease. More knowledge about the causes for engaging in online crime, both as offender and victim is also called for.

Crime-as-a-Service is a natural reflection of ordinary legal use of online services. However, when CaaS is used in conjunction with anonymity, policy makers are confronted with dilemmas concerning which crime prevention policies to pursue.

Finally, the phenomena that are new under the sun, are partially legal, partially factual. It can be questioned if criminal law de *lege lata* adequally covers *random digital crime*. There are several indications of a need for legal improvement in this respect, both as regards criminal and civil law. In fact, random digital crime seems to challenge present notions of how specific criminal provisions must be. Thus, more research on the specificity demands of the principle of legality is needed. Finally, effective filtering of sexual abuse material on the Internet should be an everlasting objective, in order to fulfil the positive obligation to make the right to private life become effective.

Sources:

Bjørkeng, P.K. (2011) *Nettkidsa – barnas digitale hverdag.* Oslo: Cappelen.

Buckels, E.E., Trapnell, P.D., and Paulhus, D.L. (2014), *Trolls just want to have Fun. Personality and Individual Differences.* 2014. Winnipeg: Elsevier.

Cybercrime Convention Committee (2013), *T-CY Guidance Notes.* T-CY(2013)29rev. Available online at www.coe.int/cybercrime.

 # 2 - Guidance Note on Provisions of the Budapest Convention covering Botnets.

 # 3 - Guidance Note on DDOS-Attacks.

 # 4 - Guidance Note on Identity Theft and Phishing in Relation to Fraud.

 # 6 - Guidance Note on New Forms of Malware.

Dagens Næringsliv (2016, January 8), *De medisinske hackerne.* Available online at http://www.dn.no/magasinet/2016/01/08/2128/Teknologi/de-medisinske-hackerne

Europol (2014), *The Internet Organised Crime Threat Assessment (iOCTA) 2014.* The Hague: European Police Office. Report available online (as per 2016).

Europol (2015), *The Internet Organised Crime Threat Assessment (iOCTA) 2015.* The Hague: European Police Office. Report available online (as per 2016).

Federal Bureau of Investigation (2016, 4 April), *FBI Warns of Business E-Mail Scams.* Available online at https://www.fbi.gov/phoenix/press-releases/2016.

Guardian (2016, May 31), *Australian Police to auction 13 million in confiscated Bitcoins* Available online at https://www.theguardian.com/technology/2016/may/31/australian-police-to-auction-13m-in-confiscated-bitcoins

(2015, April 9) *French TV Network TV5Monde Hijaced by Pro ISIS Hackers. Available online at* https://www.theguardian.com/world/2015/apr/09/french-tv-network-tv5monde-hijacked-by-pro-isis-hackers

Independent (2015, June 10) *TV5Monde Hack –'Jihadist' Cyberattack on French TV station could have Russian Link. Available online at* http://www.independent.co.uk/news/world/europe/tv5monde-hack-jihadist-cyber-attack-on-french-tv-station-could-have-russian-link-10311213.html

Interpol (2015, March 10), *Interpol Cyber Research Agenda.* Workshop Report.

Krebs on Security (2016, 16 April), *CEO Fraud.* Available online at http://krebsonsecurity.com/tag/ceo-fraud/.

McQuade, S. C. (2006), *Understanding and Managing Cybercrime.* Boston: Pearson.

Meiklejohn, S., Pomarole, M., Jordan, G. et al. (2013), *A Fistful of Bitcoin: Characterizing Payments Among Men with No Names.* Barcelona: IMC'13.

Metodekontrollutvalget (2009), NOU 2009: 15 Skjult informasjon – Åpen kontroll.

Sunde, I. M. (2006), *Lov og rett i Cyberspace.* Bergen: Fagbokforlaget.

Sunde, I. M. (2011), *Automatisert inndragning.* Complex, 3/11. Oslo: Unipub.

Sunde, I. M. (2016), *Datakriminalitet.* Bergen: Fagbokforlaget.

Wall, D.S. (2007), *Cybercrime: The Transformation of Crime in the Information Age.* UK: Wiley.

Wall, D. S. (2014), *Policing Identity Crimes.* In Wall, D. S. and Williams, M. L. (Eds.) (2014) *Policing Cybercrime,* pp. 29-52. Abingdon: Routledge.